Homework #13

1. a) Suppose $n \in \mathbb{N}$ and $n \equiv 3 \pmod 4$. Show that there is a prime p such that $p \equiv 3 \pmod 4$ and $p \mid n$.

   b) Prove that there are infinitely many primes p such that $p \equiv 3 \pmod 4$.

2. Prove the second half of the Fundamental Theorem of Arithmetic, that prime factorizations are unique. That is, prove the following statement. (You may use the fact that prime factorizations exist, since we proved this previously. You may also use Euclid's lemma.)

   For all $n \in \mathbb{N}$, if $n = p_1 p_2 \cdots p_k$ and $n = q_1 q_2 \cdots q_l$ are two prime factorizations of n, such that $p_1 \leq p_2 \leq \ldots \leq p_k$ and $q_1 \leq q_2 \leq \ldots \leq q_l$ (i.e. the primes in each factorization are written in ascending order), then $k = l$ and for all $i \in [k]$ we have $p_i = q_i$.

3. a. Let $d = \gcd(1819, 3587)$. Find d using the Euclidean algorithm.

   b. Use the extended Euclidean algorithm to find $x, y \in \mathbb{Z}$ such that $1819x + 3587y = d$.

4. Find all solutions $x \in \mathbb{Z}$ to the following congruences, or say why none exist.

   i. $5x \equiv 1 \pmod{12}$.

   ii. $6x \equiv 1 \pmod{27}$.

   iii. $56x \equiv 4 \pmod{210}$.